PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 7 : G07F 7/10

A1

(11) Numéro de publication internati nale: **WO 00/30048**

(43) Date de publication internationale: 25 mai 2000 (25.05.00)

(21) Numéro de la demande internationale: PCT/FR99/02692

(22) Date de dépôt international: 4 novembre 1999 (04.11.99)

(30) Données relatives à la priorité:
98/14224 12 novembre 1998 (12.11.98) FR

(71) Déposant *(pour tous les Etats désignés sauf US)*: GEMPLUS S.C.A. [FR/FR]; Avenue du Pic de Bertagne, Parc d'Activités de Gémenos, F–13881 Gémenos Cedex (FR).

(72) Inventeur; et

(75) Inventeur/Déposant *(US seulement)*: COOREMAN, Pascal [FR/FR]; Les Jardins de l'Infante, 23, avenue Beau Pin, F–13008 Marseille (FR).

(74) Mandataire: NONNENMACHER, Bernard; Gemplus S.C.A., Av. du Pic de Bertagne, Parc d'Activités de Gémenos, F–13881 Gémenos Cedex (FR).

(81) Etats désignés: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, brevet ARIPO (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Publiée

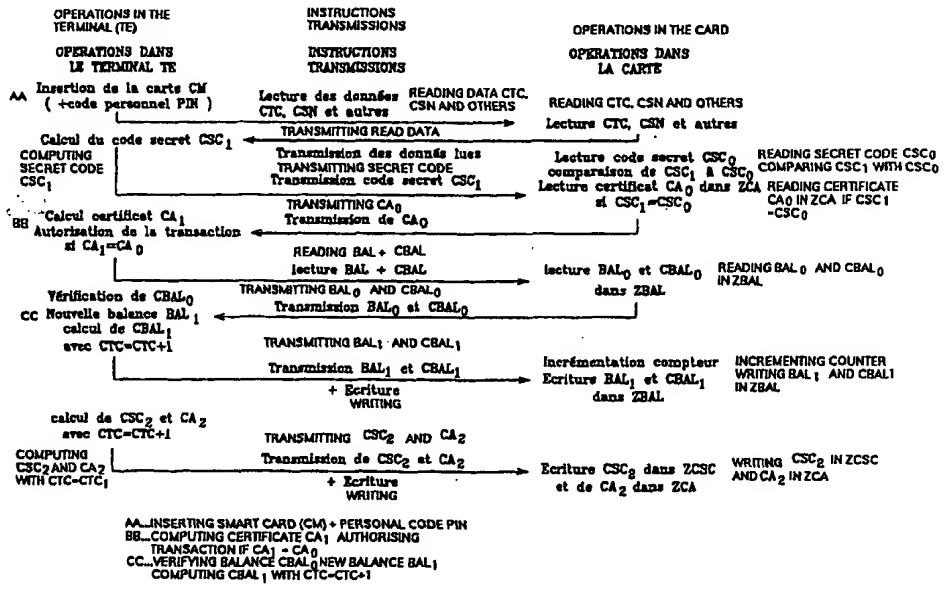
Avec rapport de recherche internationale.

(54) Title: AUTHENTICATING METHOD BETWEEN A SMART CARD AND A TERMINAL

(54) Titre: PROCEDE D'AUTHENTIFICATION ENTRE UNE CARTE A MEMOIRE ET UN TERMINAL

(57) Abstract

The invention concerns a method enabling a smart card and a terminal whereto it is connected to authenticate each other. The invention is characterised in that at the end of each transaction the terminal calculates, from data representing the card at said transaction end, a secret code CSC_2 which is recorded in a zone ZCSC with unprotected access in the card memory and an authentication certificate CA_2 which is recorded in a zone ZCA with protected access of the memory by presenting a secret code CSC_2. At the next transaction, the terminal calculates, by means of data contained in the card, a secret code and an authentication certificate which are compared to those previously recorded to perform authentication. The invention is applicable to smart cards.



(57) **Abrégé**

L'invention concerne un procédé qui permet à une carte à mémoire et à un terminal auquel elle est connectée de s'authentifier mutuellement. L'invention réside dans le fait qu'à la fin de chaque transaction le terminal calcule, à partir d'informations représentatives de la carte à cette fin de transaction, un code secret CSC_2 qui est enregistré dans une zone ZCSC à accès non protégé de la mémoire de la carte et un certificat d'authentification CA_2 qui est enregistré dans une zone ZCA à accès protégé de la mémoire par la présentation du code secret CSC_2. A la transaction suivante, le terminal calcule, à l'aide des informations contenues dans la carte, un code secret et un certificat d'authentification qui sont comparés à ceux précédemment enregistrés pour réaliser l'authentification. L'invention est applicable aux cartes à mémoire.

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	ES	Espagne	LS	Lesotho	SI	Slovénie
AM	Arménie	FI	Finlande	LT	Lituanie	SK	Slovaquie
AT	Autriche	FR	France	LU	Luxembourg	SN	Sénégal
AU	Australie	GA	Gabon	LV	Lettonie	SZ	Swaziland
AZ	Azerbaïdjan	GB	Royaume-Uni	MC	Monaco	TD	Tchad
BA	Bosnie-Herzégovine	GE	Géorgie	MD	République de Moldova	TG	Togo
BB	Barbade	GH	Ghana	MG	Madagascar	TJ	Tadjikistan
BE	Belgique	GN	Guinée	MK	Ex-République yougoslave de Macédoine	TM	Turkménistan
BF	Burkina Faso	GR	Grèce			TR	Turquie
BG	Bulgarie	HU	Hongrie	ML	Mali	TT	Trinité-et-Tobago
BJ	Bénin	IE	Irlande	MN	Mongolie	UA	Ukraine
BR	Brésil	IL	Israël	MR	Mauritanie	UG	Ouganda
BY	Bélarus	IS	Islande	MW	Malawi	US	Etats-Unis d'Amérique
CA	Canada	IT	Italie	MX	Mexique	UZ	Ouzbékistan
CF	République centrafricaine	JP	Japon	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Pays-Bas	YU	Yougoslavie
CH	Suisse	KG	Kirghizistan	NO	Norvège	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	République populaire démocratique de Corée	NZ	Nouvelle-Zélande		
CM	Cameroun			PL	Pologne		
CN	Chine	KR	République de Corée	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Roumanie		
CZ	République tchèque	LC	Sainte-Lucie	RU	Fédération de Russie		
DE	Allemagne	LI	Liechtenstein	SD	Soudan		
DK	Danemark	LK	Sri Lanka	SE	Suède		
EE	Estonie	LR	Libéria	SG	Singapour		

PROCEDE D'AUTHENTIFICATION ENTRE UNE CARTE A MEMOIRE ET UN TERMINAL

L'invention concerne les cartes à mémoire et les terminaux auxquels elles sont susceptibles d'être connectées de temps à autre et, plus particulièrement, un procédé qui permet à la carte à mémoire et au terminal de s'authentifier.

Les cartes à mémoire, du fait qu'elles ne comportent pas un microprocesseur, ne peuvent pas mettre en oeuvre un algorithme d'authentification qui implique des calculs. Cependant, certaines cartes à mémoire mettent en oeuvre un algorithme sous forme câblée qui permet l'authentification dite "active" de la carte par le terminal mais pas l'authentification inverse du terminal par la carte. Par suite de leur faible coût, les cartes à mémoire sont très utilisées dans de nombreuses applications telles que les cartes de fidélité, les contrôles d'accès, les paiements privatifs, etc ... . Cependant, par suite de l'absence d'authentification, leur sécurité d'emploi est vulnérable de sorte qu'on leur préfère parfois des cartes à microprocesseur pour certaines applications. Mais ces cartes à microprocesseur sont d'un coût nettement plus élevé, d'autant plus élevé que l'algorithme d'authentification est élaboré, ce qui conduit à les écarter pour des applications bon marché. Aussi, le but de la présente invention est d'obtenir la sécurité d'emploi des cartes à mémoire.

Ce but est atteint en mettant en oeuvre un procédé d'authentification dans lequel tous les calculs algorithmiques sont effectués par le terminal auquel la carte à mémoire est connectée.

Par ailleurs, les opérations relatives à l'authentification sont ffectuées avant le début d'une transaction proprement dite et après la fin de cette transaction en vue de l'authentification au début de la transaction suivante.

L'invention concerne donc un procédé d'authentification entre une carte à mémoire comportant au moins un compteur et un terminal, caractérisé en ce qu'il comprend les étapes suivantes consistant à :

(a) Insérer la carte à mémoire dans le terminal,

(b) Calculer dans le terminal un code secret CSC_1 selon une fonction cryptographique F de plusieurs variables comprenant au moins un code CSN identifiant la carte à mémoire et la valeur dudit compteur,

(c) Authentifier le terminal par la carte lorsque le code secret calculé CSC_1 est identique à un code CSC_0 enregistré dans la mémoire à la fin de la précédente authentification selon l'opération (f) ci-après,

(d) exécuter la transaction prévue et modifier la valeur dudit compteur,

(e) calculer dans le terminal un nouveau code secret CSC_2 selon la fonction cryptographique F du code CSN identifiant la carte à mémoire et de la nouvelle valeur dudit compteur,

(f) mettre à jour la carte à mémoire pour la prochaine transaction en enregistrant dans la mémoire, le nouveau code secret CSC_2 calculé par l'opération (e).

Pour obtenir l'authentification de la carte par le terminal, le procédé comprend les étapes supplémentaires suivantes entre les étapes (c) et (d) consistant à :

(x) calculer dans le terminal un certificat d'authentification CA_1 selon une fonction cryptographique G de plusieurs variables comprenant au moins le code CSN identifiant la carte à mémoire et la valeur dudit compteur,

(y) authentifier la carte par le terminal lorsque le certificat d'authentification calculé CA_1 est identique à un certificat CA_0 calculé et enregistré dans la carte à la fin de la précédente transaction selon les étapes (e') et (f') ci-après :

- en ce que l'étape (e) est complétée par l'étape suivante consistant à :

  (e') calculer dans le terminal un nouveau certificat d'authentification CA_2 selon la fonction cryptographique G,

- et en ce que l'étape (f) est complétée par l'étape suivante consistant à :

  (f') mettre à jour la carte à mémoire pour la prochaine transaction en enregistrant dans la mémoire le nouveau certificat d'authentification CA_2 calculé selon l'étape (e').

D'autres caractéristiques et avantages de la présente invention apparaîtront à la lecture de la description suivante d'un exemple particulier de réalisation, ladite description étant faite en relation avec le dessin joint dans lequel :

- la figure 1 est un schéma simplifié d'une carte à mémoire, et
- la figure 2 est un diagramme montrant les opérations effectuées entre le terminal et la carte à mémoire lors d'une transaction.

Le procédé de l'invention s'applique (figure 1) à une carte à mémoire CM qui comprend bien entendu une mémoire M mais aussi un compteur CT dit de transactions qui compte les transactions effectuées entre la carte

CM et un terminal TE auquel la carte est connectée par insertion.

La carte à mémoire CM peut aussi comprendre un deuxième compteur CE dit d'authentification qui compte les demandes d'authentification, ces demandes d'authentification pouvant intervenir à tout moment lors d'une transaction et indépendamment de cette dernière.

Ces deux compteurs CE et CT peuvent faire partie de la mémoire M selon des dispositifs connus.

En outre, la mémoire M de la carte comprend une première zone à accès non protégé en lecture dans laquelle est enregistré, par exemple le numéro de série CSN de la carte dans une partie ZCSN, et une deuxième zone à accès protégé pour le reste de la mémoire, cette deuxième zone comportant des parties qui sont affectées à l'enregistrement de valeurs particulières telles qu'un Certificat d'Authentification CA dans la partie ZCA et une balance BAL et son certificat d'authentification CBAL dans la partie ZBAL.

Une troisième zone ZCSC est réservée à l'enregistrement d'un code secret CSC et son accès pour enregistrement est soumis à la présentation du code secret CSC.

La mémoire M est adressée par un circuit d'adressage ADR et la transmission bilatérale des signaux entre le terminal TE et la carte CM s'effectue par l'intermédiaire d'un circuit interface INT.

Par ailleurs, la carte comprend un comparateur CP qui compare le code CSC lu dans la partie ZCSC à un code fourni par le terminal TE, le résultat de la comparaison permettant ou non l'adressage de la zone protégée de la mémoire M.

Le procédé selon l'invention sera décrit dans le cadre d'une authentification mutuelle entre la carte et le terminal en mettant en oeuvre le seul compteur de

transactions CT et des fonctions cryptographiques dites à sens unique mais le procédé de l'invention peut également s'appliquer à la seule authentification du terminal par la carte, à la mise en oeuvre simultanée des deux compteurs CE et CT et de fonctions cryptographiques autres que celles à sens unique. Les différentes opérations, notamment cryptographiques, peuvent être réalisées soit dans le terminal TE, soit dans un module de sécurité, soit encore dans un dispositif distant.

De préférence, le procédé d'authentification mutuelle selon l'invention comprend les étapes suivantes consistant à :

(m) Insérer la carte CM dans le terminal TE, cette étape pouvant comporter la présentation d'un code personnel PIN de l'utilisateur de la carte,

(n) Calculer dans le terminal TE une clé de session Ks_1 en :

(n_1) lisant le numéro de série CSN de la carte CM,

(n_2) lisant le contenu CTC_1 du compteur de transactions CT de la carte CM et,

(n_3) calculant une clé de session Ks_1 selon une fonction cryptographique à sens unique F_{Ks} telle que :

$Ks_1 = F_{ks}(K_m, CSN, CTC_1)$

- K_m étant une clé-mère enregistrée dans le terminal TE,

- F_{ks} étant par exemple une fonction du type hachage,

(o) Calculer, dans le terminal TE, un code secret CSC_1 de la carte à l'aide d'une fonction cryptographique F telle que :

$CSC_1 = F(Ks_1)$,

(p) Authentifier le terminal TE par la carte CM en :

(p_1) transmettant le code secret CSC_1 à la carte CM,

(p_2) comparant dans le comparateur CP ce code secret CSC_1 à un code secret CSC_0 enregistré dans la carte CM à la fin de la précédente transaction avec la carte, et

(p_3) autorisant la suite des opérations si la comparaison indique l'identité $CSC_0 = CSC_1$ ou en la refusant dans le cas contraire ;

(q) Calculer dans le terminal TE un Certificat d'Authentification CA_1 tel que :

$CA_1 = G(Ks_1)$

- G étant une fonction cryptographique, et

(r) Authentifier la carte CM par le terminal TE en :

(r_1) lisant le contenu CA_0 de la zone ZCA de la mémoire de la carte CM,

(r_2) transmettant au terminal TE le contenu CA_0 de cette zone protégée ZCA qui correspond à un Certificat d'Authentification CA_0 calculé à la fin de la précédente transaction,

(r_3) comparant dans le terminal TE le Certificat d'Authentification calculé CA_1 au certificat CA_0, et

(r_4) autorisant la suite des opérations si la comparaison indique l'identité $CA_1 = CA_0$;

(s) Exécuter la transaction, cette transaction pouvant consister par exemple à mettre à jour une zone de mémoire ZBAL indiquant l'état du crédit ou balance BAL restant dans la carte CM en :

(s_1) lisant dans la zone ZBAL la valeur BAL_0 de la balance résultant de la transaction précédente et le certificat correspondant $CBAL_0$,

(s_2) vérifiant que le certificat $CBAL_0$ correspond bien au résultat de la fonction cryptographique telle que :

$CBAL_0 = H(K_t, BAL_0, CSN, CTC_1)$,

- K_t étant une clé de transaction,

(s_3) incrémentant le compteur de transactions à la valeur $(CTC_1 + 1) = CTC_2$

(s_4) enregistrant la nouvelle balance BAL_1 dans la zone ZBAL,

(s_5) calculant un Certificat $CBAL_1$ de la nouvelle balance BAL_1 telle que :

$CBAL_1 = H(K_t, BAL_1, CSN, CTC_2)$, et

(s_6) enregistrant $CBAL_1$ dans la zone ZBAL ;

(t) Mettre à jour la carte CM pour la prochaine transaction avec un nouveau code secret CSC_2 et un nouveau certificat CA_2, en

(t_1) calculant dans le terminal TE :

- la future clé de session Ks_2 telle que :

$Ks_2 = F(K_m, CSN, CTC_2)$

- le futur code secret CSC_2 tel que :

$CSC_2 = F(Ks_2)$,

- le futur certificat d'authentification CA_2 tel que :

$CA_2 = G(Ks_2)$,

(t_2) enregistrant le code secret CSC_2 dans la mémoire M de la carte CM dans la zone protégée et le certificat d'authentification CA_2 dans la zone protégée ZCA.

L'invention a été décrite avec un exemple particulier de réalisation dans lequel la transaction est une opération sur la valeur balance de la carte ; cependant, l'invention s'applique à toute autre transaction selon les applications prévues pour la carte considérée.

Dans cet exemple particulier, la transaction se termine par une incrémentation du compteur de transactions CT à une valeur CTC_2 qui est égale habituellement à $(CTC_1 + 1)$. Cependant, cette valeur de CTC_2 peut être

différente de (CTC_1 + 1) et être égale, par exemple, à (CTC_1 + 3).

Ce compteur de transactions doit être incrémenté ou décrémenté à chaque transaction même si l'opération conduit à ne pas changer la balance ; dans ce cas, il faut effectuer la transaction en réenregistrant la balance inchangée mais le certificat $CBAL_1$ sera différent car le compteur de transactions aura été incrémenté. Il en sera de même du nouveau code secret CSC_2 et du certificat CA_2.

Les variables des fonctions F, G et F_{ks} qui ont été retenues dans l'exemple sont la clé-mère, le numéro de série CSN et la valeur CTC du compteur de transactions. Cependant, des variables additionnelles peuvent être utilisées telles que le code personnel PIN de l'utilisateur de la carte, ce code étant entré dans le terminal après insertion de la carte.

L'invention a été décrite dans le cadre d'une authentification mutuelle carte/terminal mais elle s'applique de manière plus générale d'abord à une authentification du terminal par la carte, cette première authentification pouvant être suivie ou non par une authentification de la carte par le terminal, l'ensemble des deux authentifications réalisant une authentification mutuelle.

L'exemple décrit utilise des fonctions cryptographiques F, G et F_{ks} utilisant des variables telles qu'une clé-mère K_m, une clé de session K_s et une clé de transaction K_t, mais de telles clés ne sont pas nécessaires pour mettre en oeuvre l'invention.

La valeur du compteur d'authentifications CE est de préférence utilisée pour le calcul du code secret CSN tandis que la valeur du compteur de transactions CT est de préférence utilisée pour le calcul du certificat d'authentification CA.

REVENDICATIONS

1. Procédé d'authentification entre une carte à mémoire (CM) comportant au moins un compteur (CE, CT) et un terminal (TE), caractérisé en ce qu'il comprend les étapes suivantes consistant à :

(a) Insérer la carte à mémoire (CM) dans le terminal (TE),

(b) Calculer dans le terminal un code secret CSC_1 selon une fonction cryptographique F de plusieurs variables comprenant au moins un code CSN identifiant la carte à mémoire et la valeur (CTE_1, CTC_1) dudit compteur (CE, CT),

(c) Authentifier le terminal par la carte lorsque le code secret calculé CSC_1 est identique à un code CSC_0 enregistré dans la mémoire à la fin de la précédente authentification selon l'opération (f) ci-après,

(d) exécuter la transaction prévue et modifier la valeur (CTE_2, CTC_2) dudit compteur (CE, CT),

(e) calculer dans le terminal (TE) un nouveau code secret CSC_2 selon la fonction cryptographique F du code CSN identifiant la carte à mémoire (CM) et de la nouvelle valeur (CTE_2, CTC_2) dudit compteur (CE, CT),

(f) mettre à jour la carte à mémoire (CM) pour la prochaine transaction en enregistrant dans la mémoire (M), le nouveau code secret CSC_2 calculé par l'opération (e).

2. Procédé selon la revendication 1, caractérisé :

- en ce qu'il comprend les étapes supplémentaires suivantes entre les étapes (c) et (d) consistant à :

(x) calculer dans le terminal (TE) un certificat d'authentification CA_1 selon une fonction cryptographique G de plusieurs variables comprenant au moins le code CSN identifiant la carte à mémoire et la valeur (CTE_1, CTC_1) du compteur (CE, CT),

(y) authentifier la carte (CM) par le terminal (TE) lorsque le certificat d'authentification calculé CA_1 est identique à un certificat CA_0 calculé et enregistré à la fin de la précédente transaction selon les étapes (e') et (f') ci-après :

- en ce que l'étape (e) est complétée par l'étape suivante consistant à :

  (e') calculer dans le terminal (TE) un nouveau certificat d'authentification CA_2 selon la fonction cryptographique G du code CSN identifiant la carte à mémoire et de la nouvelle valeur (CTE_2, CTC_2) dudit compteur (CE, CT),

- et en ce que l'étape (f) est complétée par l'étape suivante consistant à :

  (f') mettre à jour la carte à mémoire (CM) pour la prochaine transaction en enregistrant dans la mémoire (M) le nouveau certificat d'authentification CA_2 calculé selon l'étape (e').

3. Procédé selon la revendication 1, caractérisé :

- en ce que l'étape (b) consiste à :

  - calculer d'abord dans le terminal (TE) une clé de session K_{s1} selon une fonction cryptographique F_{Ks} de plusieurs variables comprenant au moins une clé-mère K_m connue du terminal (TE), le code CSN identifiant la carte à mémoire (CM) et la valeur (CTE_1, CTC_1) dudit compteur (CE, CT),

  - calculer ensuite dans le terminal (TE) le code secret CSC_1 selon la fonction cryptographique F de la clé de session K_{s1},

- en ce que l'étape (e) consiste à :
  - calculer d'abord dans le terminal (TE) une nouvelle clé de session K_{S2} selon la fonction cryptographique F_{ks} avec la nouvelle valeur (CTE_2, CTC_2) dudit compteur (CE, CT),
  - calculer ensuite dans le terminal (TE) le nouveau code secret CSC_2 selon la fonction cryptographique F de la nouvelle clé de session K_{S2}.

4. Procédé selon la revendication 2 et 3, caractérisé en ce que :
- l'étape (e') consiste à calculer le nouveau certificat d'authentification CA_2 selon la fonction cryptographique G de la nouvelle clé de session K_{S2}.

5. Procédé selon l'une quelconque des revendications précédentes 1 à 4, dans son application à une carte à mémoire (CM) comprenant deux compteurs, l'un (CE) comptant les authentifications et l'autre (CT) comptant les transactions de paiement, caractérisé en ce que les variables des fonctions cryptographiques F, G et F_{ks} comprennent les valeurs (CTE_1, CTE_2, CTC_1, CTC_2) desdits compteurs.

6. Procédé selon l'une des revendications précédentes caractérisé en ce que les fonctions cryptographiques F, G et F_{ks} sont des fonctions à sens unique.

7. Procédé selon la revendication 6, caractérisé en ce que les fonctions cryptographiques F, G et F_{ks} sont des fonctions de "hachage".

8. Procédé selon l'une des revendications précédentes 3 à 7, caractérisé en ce que l'étape (b) comprend les étapes suivantes consistant à :

(b_1) lire le numéro de série CSN de la cart (CM),

(b_2) lire le contenu (CTE_1 et/ou CTC_1) du compteur, et

(b_3) calculer la clé de session selon une fonction cryptographique F_{ks} telle que :

$Ks_1 = F_{ks}(K_m, CSN, CTC_1)$.

9. Procédé selon l'une des revendications 1 à 8, caractérisé en ce que l'étape (c) comprend les étapes suivantes consistant à :

(c_1) transmettre le code secret CSC_1 à la carte CM,

(c_2) comparer dans la carte ce code secret CSC_1 à un code secret CSC_0 enregistré dans la carte CM à la fin de la précédente transaction avec la carte, et

(c_3) autoriser la suite des opérations si la comparaison indique l'identité $CSC_0 = CSC_1$ ou en la refusant dans le cas contraire.

10. Procédé selon l'une des revendications 2 à 9, caractérisé en ce que l'étape (y) comprend les étapes suivantes consistant à :

(y_1) lire le contenu CA_0 de la zone ZCA de la mémoire de la carte CM,

(y_2) transmettre au terminal (TE) le contenu CA_0 de cette zone ZCA qui correspond à un Certificat d'Authentification CA_0 calculé à la fin de la précédente transaction,

(y_3) comparer dans le terminal TE le Certificat d'Authentification calculé CA_1 au certificat CA_0, et

(y_4) autoriser la suite des opérations si la comparaison indique l'identité $CA_1 = CA_0$.

11. Procédé selon l'une des revendications 1 à 10, caractérisé en ce que l'étape (d) comprend, dans le cas d'une modification de la balance BAL_0, les étapes suivantes consistant à :

(d_1) lire dans une zone ZBAL de la mémoire (M) la valeur BAL_0 de la balance résultant de la transaction précédente et le certificat correspondant $CBAL_0$, et

(d_2) vérifier que le certificat $CBAL_0$ correspond bien au résultat de la fonction cryptographique telle que :

$CBAL_0 = H (K_t, BAL_0, CSN, CTC_1)$,

- K_t étant une clé de transaction,

(d_3) incrémenter le compteur de transactions à la valeur $(CTC_1 + 1) = CTC_2$

(d_4) enregistrer la nouvelle balance BAL_1 dans la zone ZBAL,

(d_5) calculer un Certificat $CBAL_1$ de la nouvelle balance BAL_1 telle que :

$CBAL_1 = H(K_t, BAL_1, CSN, CTC_2)$, et

(d_6) enregistrer $CBAL_1$ dans la zone ZBAL.

12. Procédé selon l'une des revendications précédentes 1 à 11, caractérisé en ce que :

- l'étape (a) comprend en outre une étape d'entrée du code personnel PIN de l'utilisateur.

13. Procédé selon l'une des revendications précédentes 3 à 12, caractérisé en ce que :

- dans l'étape (b), l'une des variables utilisées pour le calcul de session Ks_1 est le code personnel PIN de l'utilisateur.

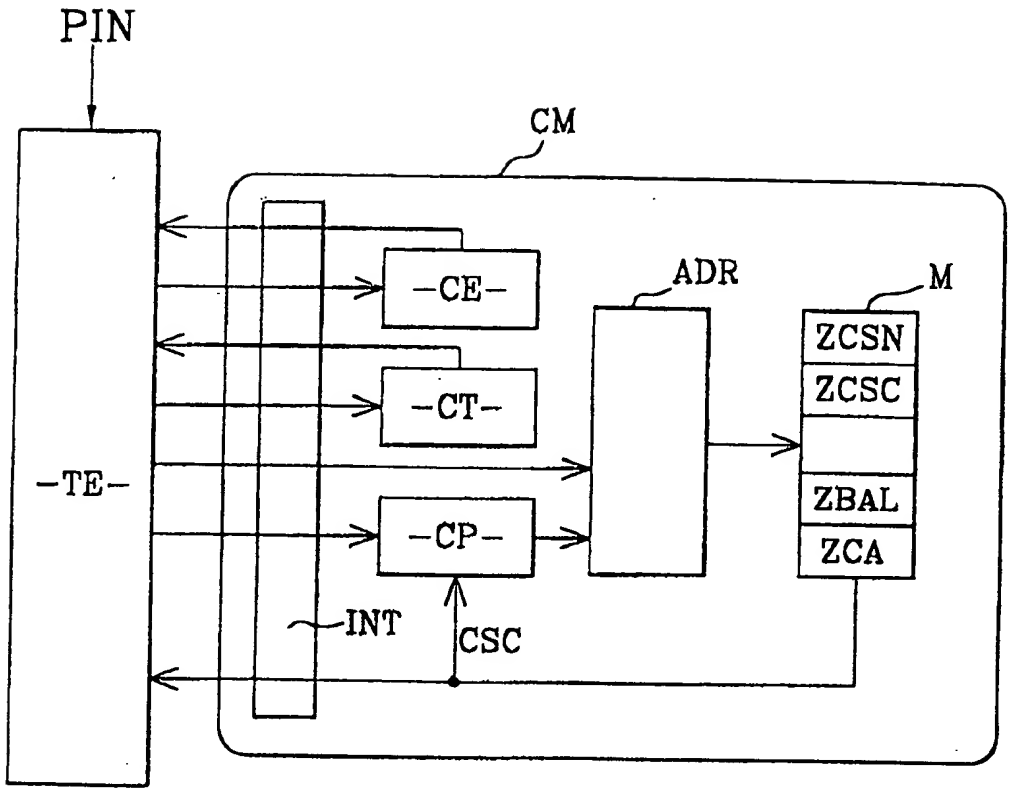


FIG.1

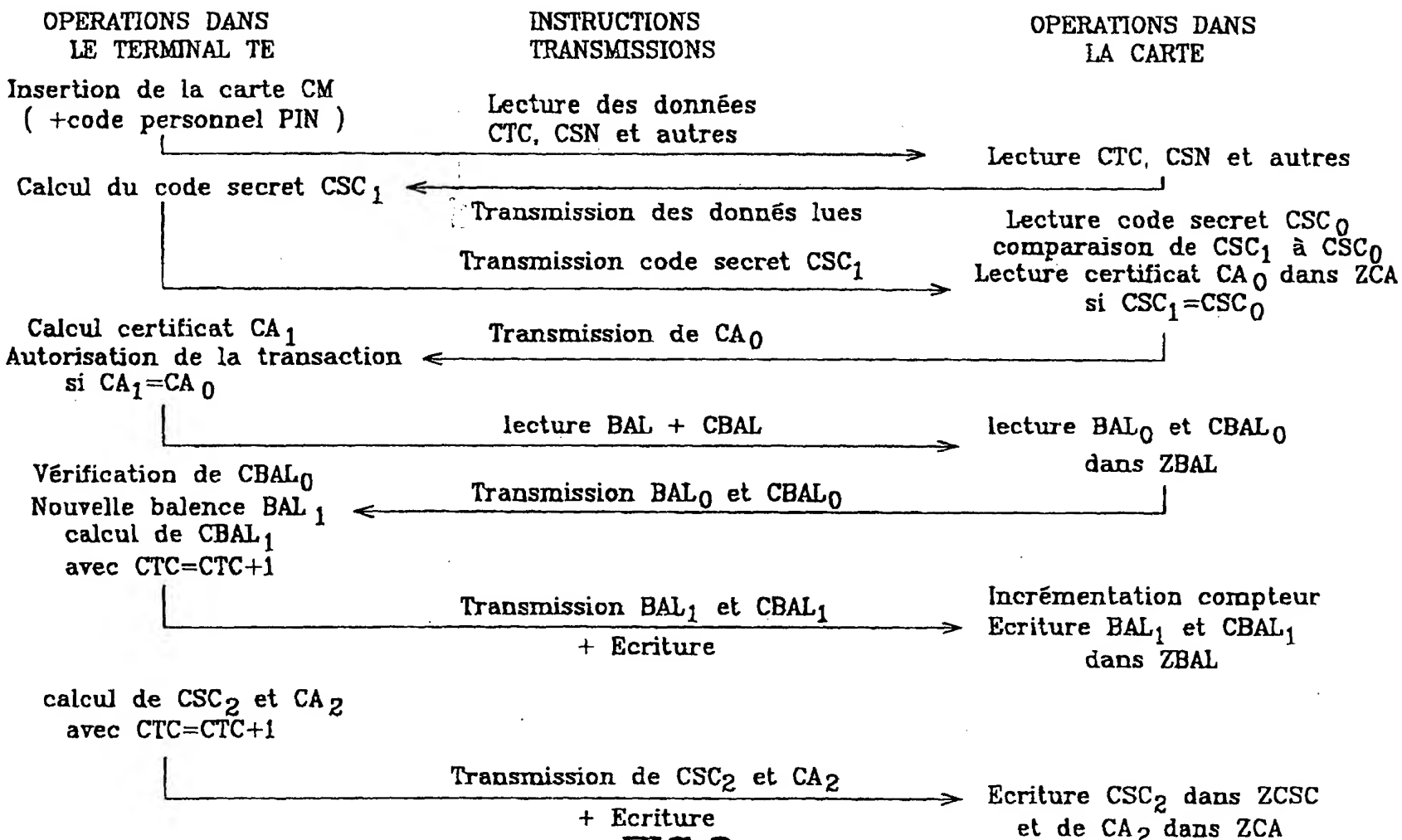

OPERATIONS DANS LE TERMINAL TE
INSTRUCTIONS TRANSMISSIONS
OPERATIONS DANS LA CARTE
Insertion de la carte CM (+code personnel PIN)
Lecture des données CTC, CSN et autres
Lecture CTC, CSN et autres
Calcul du code secret CSC1
Transmission des donnés lues
Lecture code secret CSC0
comparaison de CSC1 à CSC0
Transmission code secret CSC1
Lecture certificat CA0 dans ZCA
si CSC1=CSC0
Calcul certificat CA1
Autorisation de la transaction
si CA1=CA0
Transmission de CA0
lecture BAL + CBAL
lecture BAL0 et CBAL0
dans ZBAL
Vérification de CBAL0
Nouvelle balence BAL1
calcul de CBAL1
avec CTC=CTC+1
Transmission BAL0 et CBAL0
Transmission BAL1 et CBAL1
+ Ecriture
Incrémentation compteur
Ecriture BAL1 et CBAL1
dans ZBAL
calcul de CSC2 et CA2
avec CTC=CTC+1
Transmission de CSC2 et CA2
+ Ecriture
Ecriture CSC2 dans ZCSC
et de CA2 dans ZCA

FIG.2

INTERNATIONAL SEARCH REPORT

Int. ional Application No
PCT/FR 99/02692

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 423 035 A (GEMPLUS CARD INT) 17 April 1991 (1991-04-17) abstract; figures column 3, line 4 -column 7, line 54	1,2,11
A	EP 0 216 298 A (CASIO COMPUTER CO LTD) 1 April 1987 (1987-04-01) abstract; figures 1,4 column 5, line 6 -column 7, line 25	1,2
A	FR 2 685 520 A (MONETEL) 25 June 1993 (1993-06-25) abstract; figures page 3, line 1 -page 7, line 36	1,2,11

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 January 2000	10/02/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Buron, E

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inte .onal Application No
PCT/FR 99/02692

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document. with indication,where appropnate. of the relevant passages	Relevant to claim No.
A	WO 96 24913 A (NEXUS 1994 LTD) 15 August 1996 (1996-08-15) abstract; figure 5 page 19, line 5 -page 20, line 17	1
A	FR 2 600 188 A (BULL CP8) 18 December 1987 (1987-12-18)	

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int. ional Application No
PCT/FR 99/02692

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0423035 A	17-04-1991	FR 2653248 A	19-04-1991
		CA 2027344 A,C	14-04-1991
		DE 69014817 D	19-01-1995
		DE 69014817 T	22-06-1995
		ES 2066169 T	01-03-1995
		JP 1884135 C	10-11-1994
		JP 3241463 A	28-10-1991
		JP 6009051 B	02-02-1994
		KR 147360 B	01-12-1998
		US 5191193 A	02-03-1993
EP 0216298 A	01-04-1987	JP 2033382 C	19-03-1996
		JP 7062862 B	05-07-1995
		JP 62065168 A	24-03-1987
		US 4746788 A	24-05-1988
FR 2685520 A	25-06-1993	NONE	
WO 9624913 A	15-08-1996	NONE	
FR 2600188 A	18-12-1987	NONE	

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/FR 99/02692

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G07F7/10

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultee (système de classification suivi des symboles de classement)
CIB 7 G07F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	EP 0 423 035 A (GEMPLUS CARD INT) 17 avril 1991 (1991-04-17) abrégé; figures colonne 3, ligne 4 -colonne 7, ligne 54	1,2,11
A	EP 0 216 298 A (CASIO COMPUTER CO LTD) 1 avril 1987 (1987-04-01) abrégé; figures 1,4 colonne 5, ligne 6 -colonne 7, ligne 25	1,2
A	FR 2 685 520 A (MONETEL) 25 juin 1993 (1993-06-25) abrégé; figures page 3, ligne 1 -page 7, ligne 36	1,2,11

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
28 janvier 2000	10/02/2000

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Buron, E

1

RAPPORT DE RECHERCHE INTERNATIONALE

De le Internationale No
PCT/FR 99/02692

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	WO 96 24913 A (NEXUS 1994 LTD) 15 août 1996 (1996-08-15) abrégé; figure 5 page 19, ligne 5 -page 20, ligne 17	1
A	FR 2 600 188 A (BULL CP8) 18 décembre 1987 (1987-12-18)	

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

De ...e internationale No
PCT/FR 99/02692

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 0423035 A	17-04-1991	FR 2653248 A	19-04-1991
		CA 2027344 A,C	14-04-1991
		DE 69014817 D	19-01-1995
		DE 69014817 T	22-06-1995
		ES 2066169 T	01-03-1995
		JP 1884135 C	10-11-1994
		JP 3241463 A	28-10-1991
		JP 6009051 B	02-02-1994
		KR 147360 B	01-12-1998
		US 5191193 A	02-03-1993
EP 0216298 A	01-04-1987	JP 2033382 C	19-03-1996
		JP 7062862 B	05-07-1995
		JP 62065168 A	24-03-1987
		US 4746788 A	24-05-1988
FR 2685520 A	25-06-1993	AUCUN	
WO 9624913 A	15-08-1996	AUCUN	
FR 2600188 A	18-12-1987	AUCUN	